REMARKS

In the Official Action mailed on **07 August 2008**, the Examiner reviewed claims 1-6, 8-14, 16-22 and 24. Examiner rejected claims 1, 4-6, 8-9, 12-14, and 16 under 35 U.S.C. § 102(e) based on De Vries (U.S. Patent No. 6,928,428, hereinafter "De Vries"). Examiner rejected claims 2, and 10 under 35 U.S.C. § 103(a) based on De Vries, and the term dictionary in Javvin. Examiner rejected claims 2, and 10 under 35 U.S.C. § 103(a) based on De Vries, in view of Turvey (U.S. Patent Application No. 2002/0019849, hereinafter "Turvey"). Examiner rejected claims 3, and 11 under 35 U.S.C. § 103(a) based on De Vries, in view of Trostle (U.S. Patent No. 5,919,257, hereinafter "Trostle").

Rejections under 35 U.S.C. §103

Examiner rejected claims 3, and 11 under 35 U.S.C. § 103(a), asserting that these claims are unpatentable over De Vries in view of Trostle. Applicant respectfully disagrees, because neither De Vries, nor Trostle, nor any combination of the two, disclose (either explicitly or implicitly) a system wherein the hash of the item of private information is created by the database in a manner that is transparent to an application which manipulates the private information.

Specifically, De Vries discloses a system wherein:

> *In one embodiment of the invention illustrated herein, the black box takes the form of a set of query, answer pairs, where the query hash is represented as a hash result that is a one-way hashing function of a set of query input values. This set of query, answer pairs is distributed to other computers which can then effectively query the confidential information without having access to or directly processing the raw confidential information.* (De Vries, Col. 2, Lines 7-14)

In this system disclosed by De Vries, the **hash is calculated on a trusted computer**, and the **hash is then sent to the database** on an untrusted network. De Vries is concerned with solving the problem where untrusted providers perform queries with private information, and thus discloses a system where the private information is hashed prior to sending it to the database on the untrusted system.

In contrast to De Vries, embodiments of the present invention provide a system wherein the **hash of the item of private information is created by the database** in a manner that is transparent to an application which manipulates the private information. The present invention is not concerned that the item of private information is revealed to the database, but rather, does not want the private information stored in the database in a manner that the private information can subsequently be revealed.

Thus, De Vries teaches away from the present invention wherein the hash of the item of private information is created by the database in a manner that is transparent to an application because De Vries teaches that the private information is hashed prior to delivering it to the database.

Furthermore, Trostle discloses a system wherein:

> *During pre-boot (i.e., the period of time prior to initiating operation of the workstation operating system), a networked workstation performs an intrusion detection hashing function on selected workstation executable program(s). A computed hash value calculated by the hashing operation is compared against a trusted hash value that is downloaded from a server in order to detect illicit (i.e., authorized) changes to the selected workstation executable programs.* (Trostle, Abstract)

In this system disclosed by Trostle, a hash is created of the workstation, and is compared against a hash that is stored on a server, in order to determine if the workstation has been altered or tampered. Trostle states: "A further advantage of the present invention is that it is transparent to a user. That is, the hash function and the trusted hash value are automatically downloaded to the workstation during pre-boot, and the hashing function is automatically executed by the workstation during pre-boot to detect illicit changes to the executable files resident on the workstation." (Trostle, Col. 3, lines 23-30) Applicant avers that this is a completely different concept of "transparent" as described in the present invention.

Specifically, embodiments of the present invention are using the item of personal information as unique key. When the item of personal information is input into the application, the application then submits the item of personal information to the database to perform the lookup. The transparency comes into play here because it does not matter how the information is stored in the database, as long as the information can be converted into a form wherein records associated with the personal information can be retrieved, and as long as the information is not in a form where it can be converted back to the item of personal information. As far as the application is concerned, the item of personal information could be stored in the database in plain text (i.e. the application is unaware of the conversion). In fact, the item of personal information is used purely as a key for lookups, and is discarded by the database after the hash is created. Thus, whatever the database does to the item of personal information is transparent to the application:

> *The system then performs the query using the hash in place of the piece of private information (step 308). For example, the system can perform a "select" on the database where the hash is substituted in the "where" clause in place of the piece of private information. Note that as described previously, the hashing can take place at the database level in a manner that is transparent to the application.* (Instant Application, Paragraph [0023])

Accordingly, Applicant has amended claims 1 and 9 to clarify that the hash of the item of private information is created by the database in a manner that is transparent to an application which manipulates the private information. These amendments find support in claims 3 and 11 of the instant application. Additionally, applicant has clarified that the item of personal information is discarded after the hash is created, and the database creates an index based on the hash. Support for these amendments can be found in paragraphs [0021] and [0022] of the Instant Application. Claims 3 and 11 have been cancelled without prejudice. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1 and 9 as presently amended are in condition for allowance. Applicant also submits that claims 2, 4-6 and 8, which depend upon claim 1, and claims 10, 12-14 and 16, which depend upon claim 9, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By __/Shun Yao/______
Shun Yao
Registration No. 59,242

Date: 31 October 2008

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
FAX: (530) 759-1665
Email: shun@parklegal.com